To whom it may concern,

I am thankful for the opportunity to make this submission to the Consultation Paper.

In the Consultation Paper, it is asked:

1. In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act?
2. What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?
3. Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the *Telecommunications Act 1997* should not apply?

I do not have specific background knowledge in the field of civil proceedings to be able to answer question one or two – but as I will detail in this submission, my answer for question three is **no**, there are certainly not any kinds of civil proceedings where the prohibition should not apply.

We live in an increasingly Internet-connected modern world, and consume a vast array of services through these connections. More than ever, we leave a trace of our every action with the multiple technology providers who make these services possible. As highlighted by ABC journalist Will Ockenden in his story "*How your phone tracks your every move*"[1], the data generated as a part of providing these services can be used to expose a number of personal behaviours – such as a person's daily commuting patterns, their social connections – including how often they call particular people, where they work and live, and even an accurate guess of which flight they travel on when on holidays. Clearly, this is deeply personal and private information, and must be protected carefully. Australians enjoy some protections to their privacy, one such protection is the *Privacy Act 1988*. Of note is Australian Privacy Principle 3 – which states an organisation "*must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.*" The *Privacy Act* also allows for organisations to effectively waive the protections of the Australian Privacy Principles where required to by legislation – and this is the means by which the Data Retention legislation avoids being in violation of the *Privacy Act*.

I believe the Commonwealth Government understands that it has a duty to protect the right to privacy that every human being should be entitled to under Article 12 of the Universal Declaration of Human Rights[2] – hence it has passed legislation such as the *Privacy Act*. There are, perhaps, situations in which some individuals behave in a way that poses a serious threat to the safety or well-being of others – and in these cases the Government can justify making exceptions to the right to privacy. One such exception is to allow Data Retention legislation, despite the violation of privacy that it imposes. The reason that this violation has been somewhat accepted by the Australian public is on the grounds of national security and preventing serious criminal activity. At the time the Data Retention bill was passed, Attorney-General George Brandis said on ABC TV's Q&A: "*the mandatory metadata retention regime applies only to the most serious crime, to terrorism, to international and*

1 "How your phone tracks your every move" – ABC News, August 2015 http://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152

2 United Nations Universal Declaration of Human Rights – December 1948 https://www.un.org/en/universal-declaration-human-rights/index.html

transnational organised crime, to paedophilia, where the use of metadata has been particularly useful as an investigative tool, only to as a tool, only to crime and only to the highest levels of crime. Breach of copyright is a civil wrong. Civil wrongs have nothing to do with this scheme.[3]" The Australian public were promised that their right to privacy would only be violated under the most extraordinary criminal circumstances, and explicitly not for civil cases.

Rather than increasing access to people's private information, the Government should be taking steps to better protect it. I submit that:

- There should be no expansion of access to retained data for civil cases
- Without delay, the Government should implement a mandatory data breach notification scheme as introduced in the *Privacy Amendment (Notifiable Data Breaches) Bill 2016*[4]
- The Government should call an urgent review into the effectiveness and ethics of the Data Retention scheme

Privacy is a basic human right. Our Government should ensure that protecting this right is its highest priority. If there are any possible exceptions to this protection, it should only be in the most extreme and severe of criminal cases – and not for civil cases.

Sincerely,

Sean Lanigan

3 "National Security: Finding a Balance" – ABC TV, November 2014
http://www.abc.net.au/tv/qanda/txt/s4096883.htm

4 Privacy Amendment (Notifiable Data Breaches) Bill 2016
http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747